Information about RDHPCS Certificates

Master Certificates and Proxy Certificates

When a user first logs into a R&D HPC system, a 1-year master certificate is generated. On the next login, after the master certificate is signed, a 30-day proxy certificate is generated. Every future login renews the 30-day proxy certificate. Users need to have a valid master and proxy certificate to properly authenticate and connect to a R&D HPC system.

If you do not log into a R&D HPC system over a span of 30 days then your proxy certificate will expire and you will be require to generate a new proxy certificate. This is where the master certificate and associated passphrase is used. Users will be prompted to renew their proxy certificate by entering their passphrase (the passphrase that was created when the master certificate was generated).

If you don't remember your passphrase

Users who cannot remember their passphrase will need to enter it incorrectly 4 times (just press “Enter” 4 times) until they are prompted to also create a new master certificate. After a new master certificate is created, it will have to be signed. **Please keep in mind that this step may take a delay of 24-48 hours**. After the certificate is signed, you will receive an email telling you that you can proceed.

Generating a Master Certificate (If you have just received a RSA fob)

Each RSA fob (comes with account) is distributed with an “RSA Fob Activation” instruction sheet. Follow these instructions to set your PIN and do your first login to a R&D HPC system. You will be prompted to establish a certificate passphrase. Please read the text and follow the prompts. Your certificate passphrase must be at least 3 words. Your certificate must be signed before further access is allowed. Please allow 24-48 hours for the certificate to be signed. You will receive an email when you can proceed. After you receive the email, you will be able to log in to a R&D HPC system.

On the first login after a master certificate is generated, you will be prompted for your passphrase. **Don't worry**, you don't have to go through the signing process again. Simply enter the passphrase that you created with your master certificate, and your proxy will be renewed. After this step, you will only need your passphrase if your proxy completely expires (after 30 days).

Annual renewal of the Master Certificate

Please remember that a master certificate is valid only for one year, and has to be renewed every year as described in the previous step.

One year from the signing date of the first master certificate, a new master certificate will need to be generated. The bastion login will begin prompting you to regenerate your master certificate starting 30 days before the master certificate expires. Once the new certificate is generated, you will again have to wait 24-48 hours for the certificate to be signed, similar to your first login to a R&D HPC system.

Glossary

- **Master Certificate:** this is the certificate you get when you are prompted for your passphrase two consecutive times (once to set your passphrase, and the second time to confirm it); it has to be signed before you can login, and may have to wait for about 24 HRS before you can attempt to log in. The certificate is valid for one year. This one is common across bastions, which means there is only one certificate and is valid for one year.
- **Proxy Certificate:** this is a certificate that lasts only 30 days, but keeps getting renewed every time you login. This is local to each bastion. So you may have a valid proxy on one bastion because you use that path regularly, whereas it may have expired on the other bastion because you don't use that path often (haven't logged in for more than 30 days using that path).